

ALEX G. TSE (CABN 152348)
Acting United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

JOHN H. HEMANN (CABN 165823)
JEFFREY SHIH (MABN 663195)
Assistant United States Attorneys

SCOTT K. MCCULLOCH (DCBN 1020608)
CHRISTOPHER OTT (CABN 235659)
Trial Attorneys, National Security Division

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
john.hemann@usdoj.gov; 415.436.7478
jeffrey.shih@usdoj.gov; 415.436.7168

Attorneys for the United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,)	CASE NO. 3:17-CR-103 VC
)	
Plaintiff,)	UNITED STATES RESPONSE TO DEFENDANT'S
)	SENTENCING MEMORANDUM
v.)	
)	
KARIM BARATOV,)	Sentencing Date: April 24, 2018
)	Time: 10:30 a.m.
Defendant.)	Court: Honorable Vince Chhabria

Defendant Karim Baratov is scheduled to be sentenced on April 24, 2018. The parties agree, through the Plea Agreement and through their respective sentencing memoranda, that Probation correctly calculated the Sentencing Guidelines in the PSR. The parties and Probation also agree that the Court should impose a 24-month consecutive term of imprisonment for Counts Forty through Forty-Seven, which charge aggravated identity theft in violation of 18 U.S.C. § 1028A. There is disagreement, however, in the respective sentencing recommendations for Count One, which charges a conspiracy to commit computer fraud and abuse, in violation of 18 U.S.C. § 1030(b). For the following reasons, the

United States respectfully submits this response to the defendant's sentencing memorandum, in which he requests a sentence of 21 months for his Count One offense and relevant conduct in hacking into and selling stolen access to the webmail accounts of more than 11,000 victims.

A. Defendant Incorrectly Minimizes the Harm to His Victims

Defendant Baratov significantly understates the severity of his conduct with respect to victims to argue for a below-guidelines sentence that is inadequate for the sentencing purposes set forth in 18 U.S.C. § 3553(a). The defendant states, for example, that:

- “[h]e bore no intent to cause harm,” Def. Sent. Mem., at 3;
- “always took steps to filter his clients and targets” and that “the overwhelming amount” of his hacking to be for “Russian husbands, wives, boyfriends, and girlfriends that wanted information about their significant others,” *id.*, at 20;
- his “victims were not targeted because of their vulnerability,” *id.*, at 11; and
- “almost no victims have reported any financial harm as result of [his] conduct,” *id.*, at 12.

The Court should reject these arguments for several reasons:

First, Defendant Baratov had no reason to think that the harm he facilitated was anything but immense. The defendant did not hack in bulk. Rather, the defendant hacked specific victims that his criminal customers identified and paid the defendant to target. For every webmail account that the defendant hacked, the defendant knew his victim may have lost potentially years of personal and intimate information (*e.g.*, photographs, contacts, notes), and the passwords, tax returns, and other assorted keys and access means stored inside the hacked account. The defendant also sold his clients access to (and potentially cost his victims) the contents and control of accounts that had the same hacked password, or that used the hacked account as a recovery email address. A customer could identify such associated accounts through a review of hacked emails, and such associated accounts could include bank and other financial accounts that could be cleaned out or modified; social media accounts to be mined for information about the victim, her friends, or family; corporate email accounts of victims' employers and access to those networks. Even the \$500 proxy that he claims, incorrectly, captures the non-economic harm he caused does not really do so. No reasonable victim would provide the access Baratov stole to a criminal who had specifically targeted in exchange for the \$500 proxy loss assigned by USSG § 2B1.1. And Baratov knew well the harm that could be caused to his victims, as he himself joined in

1 exploiting the access he tricked them into providing. *See, e.g.*, Supplemental Kobzanets Decl. (filed
2 under seal on April 20, 2018) ¶ 3.d (describing defendant’s use of hacked accounts that his victims
3 abandoned); Kobzanets Decl. ¶ 2.c (defendant himself in certain instances deleted the contents of a
4 victim’s account).

5 Second, contrary to his assertion, the defendant has no idea and never considered whether his
6 victims were targeted because of a vulnerability. Def. Sent. Mem., at 11. He took orders from his
7 customers through his website to target specific victims without needing any information about the
8 victims, for example to reveal whether they were adults or children, sick or well, or any other
9 characteristics someone interested in minimizing harm might consider. He did not ask questions that
10 might have revealed particular danger, if he could have verified the answers he received (and he could
11 not). At bottom, while he may want to rationalize his conduct, he knew that he hacked into victim
12 accounts indifferently and indiscriminately. To the extent that he advertised to Russian-speakers (who
13 could be anywhere) and avoided victims with government accounts or those in the U.S. and Canada, he
14 did so to avoid getting caught, not to mitigate any harm. Supplemental Kobzanets Decl. ¶ 3.b, c.

15 Third, the defendant’ did not filter his customers and victims, as he claims, so that “the
16 overwhelming amount” of his hacking was for jealous spouses and significant others. Def. Sent. Mem.,
17 at 20. The correspondence with his customers shows that as long as he was paid, he hacked into victim
18 webmail accounts with little, if any, discussion with his customers about their identity, motives, and
19 plans. Docket No. 36 (“US Sent. Mem.”), at 4. His website did not seek to serve only those customers
20 who were jealous spouses or significant others. *Id.*, at 2-3. The defendant thus hacked for the Russian
21 Federal Security Service, and for another customer who may have provided services to hurt and kill
22 people. US Sent. Mem., at 4. Even if a customer claimed to be a jealous spouse or significant other,¹
23 the defendant would not be able to confirm such customer claims through his arms-length’s dealings and
24 his keyboard. Moreover, hacking victim accounts in the context of domestic disputes, where there could
25 be issues of domestic violence, child custody, and personal trauma, does not mitigate the harm to those
26

27 ¹ As the defendant agreed to and attempted to hack more than 80 accounts for “Patrick
28 Nag,” he could not have reasonably believed that “Patrick Nag” was a jealous individual targeting his
spouses and significant others. The same is true for defendant’s other repeat customers.

1 victims nor make the defendant's criminal conduct less severe.² *See, e.g.*, US Sent. Mem., at 7-8
 2 (summarizing Victim 3 impact).

3 Fourth, in stating that "there is little evidence to indicate that Mr. Baratov's actions resulted in
 4 serious financial loss to any of his victims" and that "only three victims that claim to have been injured
 5 by Mr. Baratov's conduct, all of which are located outside of the United States," Def. Sent. Mem. 5, 11,
 6 the defendant ignores his own impact on the victim responses. The defendant violated his victims
 7 through their email accounts (not by stealing from the victim's person or physical premises), and thus,
 8 the hacked victim accounts constitute the primary, and usually the only, identifying information for the
 9 victims. That more than 4,000 of those victims have, after being hacked, shut down their former
 10 accounts does not lessen his culpability. For those victims who continue to use the same accounts that
 11 the defendant hacked, they may not be inclined to respond to trustworthy-looking, unexpected emails
 12 and websites that ask for personal information (such as the information requested in the Victim Impact
 13 Statement). Malicious, trustworthy-looking emails are how the defendant hacked them in the first place.
 14 And as illustrated by the three victim responses that the United States did receive, US Sent. Mem., at 7,
 15 the harm suffered from the hacking of a webmail account (while immense as discussed above) is not
 16 easily reduced to a dollar amount nor easily supported by documentation.³ Indeed, the \$500 loss

18 ² The defendant also suggests — without specifically arguing — that he is less culpable
 19 because some unknown but significant portion of his victims were not U.S. citizens. *See* Def. Sent.
 20 Mem., at 5, 20. This is incorrect. Operating a sprawling international criminal business and hacking
 21 victims, including over 2,000 accounts hosted by service providers in the United States, without any
 22 discussion of identities, motives, and plans add to, rather than subtract from, culpability. Many
 23 significant hackers operate outside the United States. In the context of international hackers-for-hire,
 24 such as the defendant, the victims will be distributed around the world. The dictates of § 3553(a),
 25 especially the need for general deterrence, are not served by stating that such prolific international
 26 cybercriminals can only be held accountable for their conduct through separate prosecutions in each of
 27 the countries where the victims reside.

28 The defendant states as well that his admitted relevant conduct under USSG § 1B1.3 is
 "entirely unrelated to the instant Indictment," Def. Sent. Mem., at 5. That is incorrect. The defendant
 pleaded guilty in Count One to a computer hacking conspiracy in which the two Russian FSB officers
 hired criminal hackers to collect information through computer intrusions in the United States and
 abroad between January 2014 and December 2016. The defendant's role in that conspiracy was to spear
 phish the webmail accounts of individuals of interest to his co-conspirators and to send those account
 passwords to Co-Defendant Dokuchaev in exchange for money. The difference between his hacking
 conduct in the Count One conspiracy and his hacking of more than 11,000 victims for other customers
 (which he agrees in the Plea Agreement is relevant conduct for sentencing purposes) is just the names of
 the customers.

³ Moreover, the defendant does not have substantial assets remaining to pay restitution

imposed for Sentencing Guidelines purposes by Application Note 3(F)(i) of USSG § 2B1.1 is a reflection that the actual losses that are asserted and can be substantiated in these cases understates the harm to victims. The lack of documented losses for restitution purposes does not lessen the severity of his conduct.

B. The “Shadow Guidelines” Do Not Provide Useful Guidance or Aid Defendant

Defendant Baratov invokes the hypothetical “shadow guidelines” and asserts that this Court should impose a sentence based on his own guideline calculation under those, instead of the actual Sentencing Guidelines calculation, to which he, the United States, and Probation agreed.

The shadow guidelines have been considered and rejected by the Sentencing Commission even for use in cases their framers designed them to address.⁴ This hacking case is not one of those. Defendant Baratov purports to invoke the shadow guidelines for their focus on less “easily quantifiable” factors (quoting a District of Connecticut case, *see* Def. Sent. Mem., at 15). In fact, the shadow guidelines and Sentencing Guidelines do not lead to as large of a discrepancy as the defendant claims. The main benefit here for the defendant in urging the use of the shadow guidelines appears to be the opportunity to minimize culpability in a way that he cannot under the Sentencing Guidelines, because he agreed to a Sentencing Guidelines calculation in his Plea Agreement, in order to present a lower guideline range to the Court.⁵

claims because of his lavish spending. US Sent. Mem., at 14.

⁴ The Sentencing Commission considered the structure proposed by the ABA Task Force on the Reform of Federal Sentencing for Economic Crimes and did not adopt the shadow guidelines. In September 2013, for example, the United States Sentencing Commission held a Symposium on Economic Crime to examine and as part of a comprehensive multi-year study of the fraud guideline. Transcript of U.S. Sentencing Commission Symposium on Economic Crime, September 18-19, 2013, *available at* <https://www.ussc.gov/research/research-and-publications/research-projects-and-surveys/united-states-sentencing-commissionsymposium-economic-crime>, at pp.20-21 (Opening Remarks of the Honorable Patti B. Saris, U.S. District Court Judge and Chair of the U.S. Sentencing Commission). Among the various topics, the structure proposed in the shadow guidelines was presented and discussed. *Id.*, at pp.106-193; *see also* Plenary Session III of U.S. Sentencing Commission Symposium on Economic Crime, *available at* <https://www.ussc.gov/research/research-and-publications/research-projects-and-surveys/united-states-sentencing-commissionsymposium-economic-crime>. At the conclusion of the United States Sentencing Commission’s multi-year study, however, the shadow guidelines were not adopted. *See* Amendment 792 of USSG, Reasons for Amendment (stating that “[t]his amendment is a result of the Commission’s multi-year study of § 2B1.1 and related guidelines, and follows extensive data collection and analysis relating to economic offenses and offenders. Using this Commission data, combined with legal analysis and public comment, the Commission identified a number of specific areas where changes were appropriate.”).

⁵ Moreover, even if this Court were to consider the shadow guidelines in this case, as the

The shadow guidelines were proposed for economic crimes where dollar-loss amounts could arguably be divorced from culpability, not computer fraud and abuse crimes. As explicitly caveated by the ABA Task Force on the Reform of Federal Sentencing for Economic Crimes, “we discussed but did not fully resolve the question of whether certain categories or types of offenses should be sentenced under a separate guideline in light of the very wide array of offenses sentenced under this [shadow] guideline.” Docket No. 37-1, at 12. The ABA also explicitly caveated that “[w]e have performed no research and have no empirical basis for the levels we assigned in the draft.” Docket No. 37-1, at 12.⁶ The absence of computer fraud examples in the Case Scenarios appended to shadow guidelines similarly indicates that the ABA never calibrated its proposal to include such computer crimes. *Id.*, at 14-18.⁷

Since the shadow guidelines do not seek to alter sentences in computer fraud cases like this one, it is unsurprising that the defendant’s attempt to invoke the shadow guidelines does not much help him without other incorrect and self-serving tweaks. For example:

- For the “victim impact” score, the defendant errs in minimizing the harm to victims as discussed in the section above. Additionally, the defendant argues that when applied under the shadow guidelines, § 2B1.1’s \$500 loss proxy captures the whole, holistic analysis otherwise preferred by the shadow guidelines, mooted any further inquiry into non-economic harms—though such inquiry is the main point of the shadow guidelines—and leading to a lower recommended sentence than the Sentencing Guidelines. That is not true: defendant’s own analysis of his purported shadow guidelines range requires repeatedly minimizing non-economic harm factors

Second Circuit observed, this Court is “(to understate the case) no more bound by a hypothetical set of [Shadow G]uidelines issued by proponents of changes in the law than it was by the actual [Sentencing] Guidelines promulgated by the Sentencing Commission.” *Rivernider*, 828 F.3d 91, 114 (denying defendant’s challenge to his sentence above the shadow guidelines range, and finding defendant’s substantive unreasonableness argument as lacking “any basis in law”).

⁶ Even if the ABA had tried to calibrate the shadow guidelines to computer fraud, it is unclear how a court could take usable guidance from them. The shadow guidelines provide a range of 20 offense levels for culpability, on top of 8 offense levels for aggravating/mitigating role. That those two factors alone combine for a range of 28 offense levels, before taking into account any base offense levels or specific offense characteristics, bespeaks caution.

⁷ Even in those hacking cases closest to the financial cases, where concerns about § 2B1.1 are greatest (*e.g.*, the in-bulk “carding” cases centered on fraudulent credit card theft and transfer with dollar-loss sentence drivers), courts appear to have uniformly sentenced in reference to the Sentencing Guidelines. *See, e.g.* Sentencing Transcript in *United States v. Seleznev*, 11-CR-70, Docket No. 478, at p.44 (W.D.Wash. April 21, 2017) (sentencing defendant who led broad carding conspiracy to 27 years imprisonment, noting the importance of general deterrence, acknowledging the defendant’s difficult upbringing, and stating, “You worked hard to educate yourself in computer use. You’re to be applauded for that. That education was an opportunity to change how you dedicated yourself with that talent. Unfortunately, you elected to pursue the pathway of a fraudster. Your education was your first chance to avoid what you face today.”); Sentencing Transcript in *United States v. Gonzalez*, 08-CR- 10223 (Saris, J.), Docket No. 94, at p.36 (D.Mass Mar. 25, 2010) (sentencing defendant in broad carding conspiracy to 20 years imprisonment).

like victim vulnerability. And, the \$500 loss amount that applies for each victim in this case under Application Note 3(F)(i) of USSG § 2B1.1 is calibrated to the loss table of the Sentencing Guidelines. There is no reason to believe that the Sentencing Commission would have chosen the same amount to drive the shadow guideline table.

- For the loss enhancement under the shadow guidelines, the defendant applies the \$500 loss proxy of Application Note 3(F)(i) in USSG § 2B1.1, but understates his loss enhancement as more than \$1 million resulting in +8. Def. Sent. Mem., at 7-8. The defendant hacked into 11,000 accounts. Plea Agreement ¶ 2.d. At \$500 per account, the loss would be \$5.5 million under the shadow guidelines loss table resulting in a +10.
- For the “culpability” score, the shadow guidelines direct that the culpability factor of gain should be determined by the gain to “the defendant and others involved in the criminal undertaking.” Docket No. 37-1, at 3-4. In his shadow guidelines calculation, however, the defendant considers only the \$100 gain to himself. He does not consider the gain to any of his criminal co-conspirators, *i.e.*, customers of 11,000 hacked accounts. Def. Sent. Mem., at 9. Similarly, the shadow guidelines provide as examples of extenuating circumstances coercion or duress that could contribute to the commission of the offense. Docket No. 37-1, at 8. Instead of evaluating circumstances that may have coerced the defendant into the offense, the defendant without any authority argues that his age, lack of law enforcement contact, and focus on targets outside the United States constitute positive “extenuating circumstances.” Def. Sent. Mem., at 9-10. And without any authoritative data points, the defendant summarizes the various culpability factors to assert that he should have a shadow guidelines culpability score of zero. *Id.*, at 10.

In short, it is unclear what the shadow guidelines mean in this case, if they should mean anything at all, and the defendant is using them simply to bolster the below-guideline outcome that he desires.

None of the cases that the defendant cites for applying the shadow guidelines arise in a case of computer fraud and abuse. Instead, the cases cited by the defendant, Def. Sent. Mem. 14-15, highlight the gulf between the kinds of cases where courts have weighed the shadow guidelines, and this one. *See* Sentencing Transcript for *United States v. Faibish*, 12-CR-265, Docket No. 271 (EDNY May 13, 2016) (applying shadow guidelines where Faibish faced a Sentencing Guidelines range of life imprisonment in a dollar-loss-driven securities and bank fraud case); Sentencing Transcript in *United States v. Rivernider*, 10-CR-222, Docket No. 609, at 205 (D.Conn. Feb. 3, 2014) (stating that the reasons the shadow guidelines were preferable, in handing down 144 month sentence in a \$20 million dollar-loss-driven wire fraud case, included that the defendant’s culpability was overstated because he was not predatory and was in fact defrauded himself: “it’s important to realize that you were a victim of fraud, which distinguishes you from the predators I have known in cases involving economic crimes”); *United States v. Litvak*, 13-CR-19 (D.Conn. July 23, 2014) (securities fraud case). In addition to the differences in the types of crimes, none of the cases cited by the defendant appears to have an agreed-upon Sentencing Guidelines range pursuant to a Plea Agreement as is the case here. *See United States v.*

1 *Faibish*, 2015 WL 4637013, at *2-3 (EDNY Aug. 3, 2015) (unpublished) (taking notice of shadow
 2 guidelines in denying defendant's request for *Fatico* hearing to determine precise loss amount); Jury
 3 Verdict in *United States v. Faibish*, 12-CR-265, Docket No. 214 (indicating conviction after trial);
 4 *United States v. Rivernider*, 828 F.3d 91, 101 (2d Cir. 2016) (describing defendants' guilty pleas in after
 5 10 days of trial); Courtroom Minutes in *United States v. Rivernider*, 10-CR-222, Docket No. 365
 6 (indicating change of plea without plea agreement); Jury Verdict in *United States v. Litvak*, 13-CR-19,
 7 Docket No. 510 (indicating conviction after trial).

8 The shadow guidelines do not provide an appropriate ground for a below-guideline variance in
 9 this case, and the Court should decline to accord them any weight in sentencing the defendant.

10 **C. Defendant Cites Cases Supporting a Guideline Sentence**

11 Defendant Baratov cites the sentences in *United States v. Collins*, 16-CR-121 (M.D.Pa.), *United*
 12 *States v. Majerczyk*, 16-CR-550 (N.D.Ill.), and *United States v. Hatala*, 12-CR-912 (S.D.N.Y.) to argue
 13 that a below-guidelines sentence is necessary in this case to avoid unwarranted disparity. Def. Sent.
 14 Mem., at 15-19. All three of those defendants, though, received guideline-or-higher sentences pursuant
 15 to plea agreements. *See* Docket No. 37-2, at 3 (Collins pursuant to plea agreement); 37-4, at 3
 16 (Majerczyk pursuant to plea agreement); 37-6, at 5 (Hatala pursuant to plea agreement). In this case, as
 17 Defendant Baratov agreed in his plea agreement, the applicable Sentencing Guidelines range in his case
 18 is higher than the range of each of those cases. That is because his criminal conduct was more serious
 19 and voluminous.

20 For example, in *United States v. Ryan Collins*, 16-CR-121 (M.D.Pa. Oct. 26, 2016), the Court
 21 sentenced Collins to 18 months in prison for hacking roughly one-twentieth as many victims as the
 22 defendant, apparently to satisfy a sexual urge. The harm in that case appeared to be limited to Collins's
 23 known motives and plans for his hacking, and the Court there handed down an above-guidelines
 24 sentence. *See* Docket Nos 37-2, 37-3. In this case, the harm caused by Collins is just one of the many
 25 types of harms that could have motivated Defendant Baratov's customers.

26 In *United States v. Majerczyk*, 16-CR-550 (N.D.Ill. Feb. 6, 2017), Majerczyk hacked his 30
 27 victims for "kicks"—causing far less damage to each of his far, far fewer victims than the defendant—
 28 and received a sentence in the middle of the guideline range.

In *United States v. Hatala*, 552 Fed. Appx 28 (2d Cir. 2014), the Second Circuit affirmed an upward departure from the guideline range. Hatala was sentenced for selling “approximately 300” usernames and passwords—not 150,000. In particular, Hatala did not target specific victims on behalf of customers, and the number of 300 PayPal username/password combinations was substantiated by specific evidence that the defendant consummated the sales of those accounts. Docket No. 37-6, at 5. The 150,000 username/password combinations found in a bulk list during the investigation, however, needed to be run through “checker” software on their own to determine whether any of them, and if so, which ones, were valid. *Id.*, at 4. Even though the harm to victims in that case was less than in this one, with purely financial information taken from victims who were not singled out for targeting by criminals, the Court departed upward from the guidelines. None of these cases cited by the defendant supports the proposition that the Sentencing Guidelines that he agreed to in this case overstate the appropriate sentence under 18 U.S.C. § 3553(a).

* * *

Accordingly, in full consideration of the Sentencing Guidelines and the factors enumerated in 18 U.S.C. § 3553(a), the United States respectfully recommends that the Court impose a sentence of 70 months imprisonment for Count One, 24 months consecutive imprisonment for Counts Forty through Forty-Seven, 3 years supervised release, and restitution and fine amounts that encompass any and all of his assets.

Respectfully submitted,

ALEX G. TSE
Acting United States Attorney

DATED: April 21, 2018

/s/ Jeffrey Shih
JEFFREY SHIH
Assistant United States Attorney

SCOTT K. MCCULLOCH
Trial Attorney, National Security Division